AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Sean P. Doyle, United States Postal Inspector, being duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under Federal Rule of Criminal Procedure 41 and 18 U.S.C. §§ 2703(c)(1)(A) for information about the location of the cellular telephone assigned call number 351-322-4889, subscribed to Julio Angel Savinon, IMEI number 350928999042110 (the "TARGET CELL PHONE"), and whose service provider is Verizon Wireless ("the PROVIDER"), a wireless telephone service provider headquartered at 180 Washington Valley Road, Bedminster, NJ. The TARGET CELL PHONE is described herein and in Attachment A, and the location information to be seized is described herein and in Attachment B.
2. Because this warrant seeks the prospective collection of information, including cell-site location information, that may fall within the statutory definitions of information collected by a "pen register" and/or "trap and trace device," *see* 18 U.S.C. § 3127(3) & (4), the requested warrant is designed to also comply with the Pen Register Act. *See* 18 U.S.C. §§ 3121-3127. The requested warrant therefore includes all the information required to be included in an order pursuant to that statute. *See* 18 U.S.C. § 3123(b)(1).
3. I have been employed as a Postal Inspector by the United States Postal Inspection Service ("USPIS") since July 2016. I was assigned to the USPIS Connecticut and Western Massachusetts Major Crimes Team from 2016 through August of 2019. In August of 2019, I transferred to the USPIS Manchester, NH Prohibited Mail Narcotics/ Miscellaneous Crime Team. On these teams, my duties and responsibilities include, but

are not limited to, the investigation of the illegal shipment of narcotics and narcotics proceeds, as well as the laundering of drug proceeds via the United States Postal Service ("USPS") and the investigations of burglaries and robberies of USPS employees and facilities. Prior to becoming a U.S. Postal Inspector, I was employed for ten years as a police officer for the Town of Londonderry, New Hampshire.

4. I have received extensive training in criminal investigations, procedures, and criminal law, and I have assisted senior postal inspectors and other law enforcement agents in numerous criminal investigations, the execution of search warrants and in arrest procedures. I have received training from the USPIS in the investigation of controlled substances and proceeds/payments for controlled substances being transported through the United States Mail and training on robberies and burglaries of USPS employees and facilities. I have also received asset forfeiture training and have consulted with senior postal inspectors and asset forfeiture specialists.

5. I am a law enforcement officer of the United States within the meaning of Title 18 U.S.C. § 3061, and am empowered by law to conduct investigations and make arrests for offenses enumerated in Title 18 U.S.C. § 111(a)(1), Assaulting, resisting, or impeding certain officers or employees, Title 18 U.S.C. § 2114, Robbery of any person having lawful charge, control, or custody of any mail matter or of any money or other property of the United States, and 18 U.S.C. § 1704, Keys locks stolen or reproduced and other federal offenses.

6. The information set forth in this affidavit is based on an investigation other law enforcement agents and I are conducting. This affidavit does not contain every fact known to me with respect to this investigation. Rather, it contains those facts I believe to be necessary to establish probable cause for issuance of this arrest warrant.

GENERAL BACKGROUND CONCERNING THE UNITED STATES MAIL AND POSTAL SERVICE KEYS

7. Postal customers use blue collection boxes to send various types of U.S. Mail. First class mail is the most common type of mail sent by stamp and envelope. Some of the most common items sent in first-class mail by postal customers are checks. These checks are often placed into a U.S. Postal Service ("USPS") blue collection box on the street or at a post office. As a result, criminals routinely target USPS first-class mail placed in blue collection boxes to steal checks.

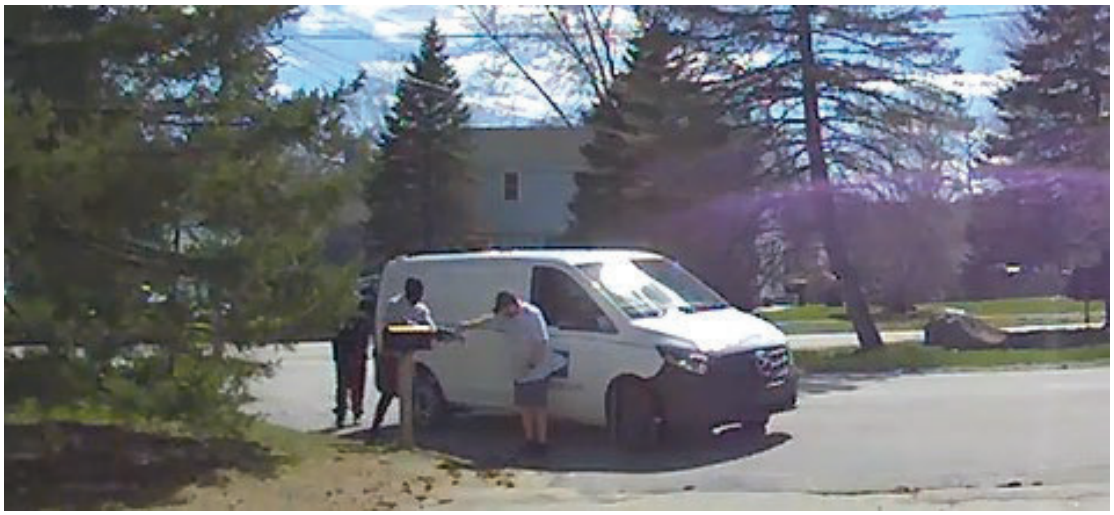
8. One method of stealing mail from a blue collection box is to obtain an "Arrow key" to unlock the box. These Arrow keys are the property of USPS and it is a federal offense (18 U.S.C. § 1704) for an unauthorized person to possess one. One method of obtaining an Arrow key is through the robbery of a postal carrier, which would constitute a violation of 18 U.S.C. §§ 111(a)(1) and 2114.

9. Criminals involved in mail theft from blue collection boxes often operate in organized groups recruited to perform specific functions. Some individuals are recruited to steal the mail, while others are recruited to provide their banking information to launder the stolen checks. These recruited account holders are often promised money in exchange for the use of their accounts.

PROBABLE CAUSE

10. Based on my investigation and that of others, including the review of witness/victim statements and surveillance videos/photos, on April 16, 2024, at approximately 2:39 PM, the Nashua, NH Police Department ("NPD") responded to Blacksmith Way, Nashua, NH for a report of an armed robbery. Information was provided that a USPS letter carrier was held at gunpoint for his Arrow Key. NPD spoke with the carrier, who stated he was

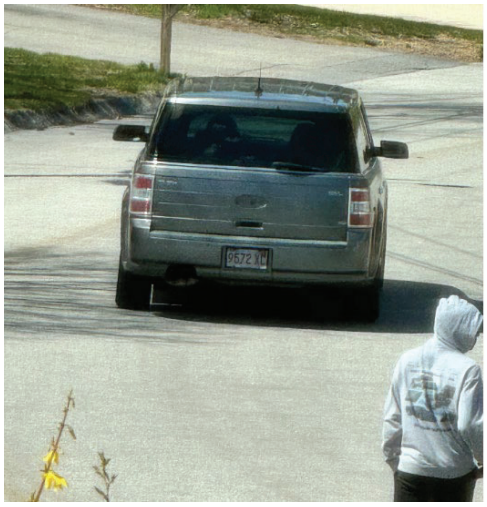
robbed after delivering mail on Blacksmith Way. The carrier described that as he was walking back to his USPS van, a dark-skinned male wearing a black-colored balaclava and a gray sweatshirt was standing near the USPS van. The carrier stated this male pointed a black firearm at his chest and demanded his "keys to the city." The carrier provided his keys to the male, which included an Arrow key. NPD was later able to obtain video surveillance from a residence, which was consistent with the carrier's account of the incident. This video surveillance also depicted a second involved male, dressed in all black, who was behind the USPS van and potentially out of view from the carrier. A screen capture of the video is incorporated herein:



11. Inspectors and NPD conducted a canvass of the area of following the incident. During the canvass, USPIS and NPD made contact with a local resident, who stated that he saw information about this incident on social media and believed he had pictures of the suspects and their vehicle. The resident stated that he saw the vehicle driving very slowly through the neighborhood and that the occupants' clothing was abnormal for the weather, given that it was a warm day and both had their hoods up over their heads. Two male occupants also entered and exited the suspect vehicle on several occasions for no

apparent purpose. After noting the behavior, the resident entered his own vehicle, followed the suspects, and photographed them and the suspect vehicle.

12. The resident provided the pictures and video to law enforcement. Some of those images are incorporated herein:



The photographs the resident provided were consistent with the two suspects seen on the video of the robbery. Through these pictures, law enforcement was able to identify the suspect vehicle as a gray-colored Ford Flex bearing Massachusetts registration 9572XC.

13. A query of Massachusetts Registration 9572XC revealed the vehicle to be registered to W.C. at a specific address in Lowell, Massachusetts. NPD and Postal Inspectors proceeded to this address along with the Lowell, MA Police Department ("LPD") in an attempt to make contact with this vehicle and its occupants. Upon doing so, law enforcement observed the Ford Flex traveling along Douglas Road in Lowell and were able to conduct a traffic stop on the vehicle on Glenellyn Street in Lowell. The driver of the vehicle was a juvenile male ("T.C."). Law enforcement contacted T.C.'s parents, one of whom was the registered owner of the Flex, who responded to the scene of the traffic stop on Glenellyn Street. Based in part on speaking with T.C., investigators identified the robbers as Baraka JANVIER and a then-juvenile ("C.V.").

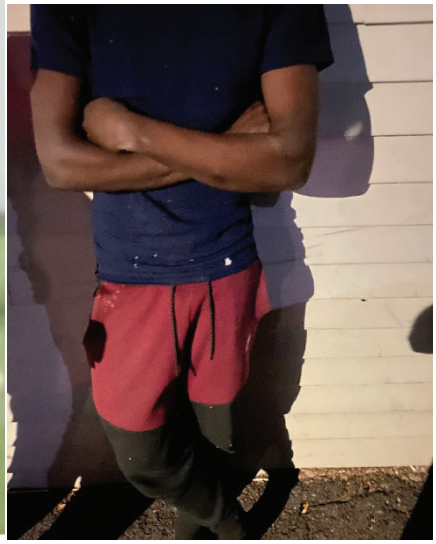
14. Law enforcement responded to 90 White Street in Lowell in an attempt to make contact with JANVIER and C.V. As law enforcement knocked and announced their presence at the front door, law enforcement in the rear of the residence heard doors and drawers being opened and closed hurriedly. Seconds after the loud noises, C.V. and JANVIER exited the rear of the building in a hurried state. Law enforcement detained C.V. and JANVIER at the rear residence outdoor stairs. Both C.V. and JANVIER were brought to the front of the building by law enforcement and separated.

15. During the contact at 90 White Street, investigators obtained consent to search the residence and a vehicle for the Arrow key and other evidentiary items. During this search, two black pistol BB guns were located concealed in a clothing dryer, at the rear of the

residence. A dark colored mask, consistent with the one worn by JANVIER during the robbery, was also located in the front seat of the vehicle.

16. In an interview, JANVIER stated that he and C.V. were driven to Nashua earlier in the day and robbed a mail carrier for a key. JANVIER stated he and C.V. met a male subject C.V. knew, in Lowell, and that after the robbery, they gave that male the key.

17. When detained by law enforcement, JANVIER was still wearing pants which were consistent with the pants he was observed wearing while committing the robbery. Photographs are incorporated herein:

18. In an interview, C.V. stated that he learned through a Telegram channel that individuals were paying for USPS Arrow keys. C.V. indicated that he and JANVIER had been transported to Nashua and JANVIER had used a BB gun to rob the mailman. C.V. admitted to being with JANVIER when he robbed the mailman. C.V. stated they were after the "key."

19. C.V. advised that he and JANVIER went to the area of "Family Dollar," later determined to be the Dollar Tree, on Newhall St. in Lowell, MA to sell the Arrow key for $15,000. C.V. then changed his story to say that he met the buyer for the key identified as "Ty" at

Olivera Park, on Newhall St. in Lowell, MA to sell the Arrow key. C.V. described "Ty" as a Hispanic male, with curly hair, skinny, 5'7," wearing light blue jeans, a "Bape" hooded sweatshirt and a Louis Vuitton messenger bag.

20. C.V. stated that he believed that "Ty" was going to keep the key and use it for financial crime. C.V. stated "Ty" was going to attempt to use the Arrow key on the night of the robbery to confirm its validity. If the key worked, "Ty" was going to meet with C.V. and JANVIER to pay them for the key.

21. C.V. provided consent to search his cell phone. During a review of C.V.'s phone, "Ty" was determined to have a Telegram username of @T5xyy, an Instagram handle of T5xyy, and a phone number of 351-322-4889. A search of CLEAR, a paid law enforcement database, which has proven reliable in previous investigations, identified that phone as being operated by Verizon Wireless. C.V. stated that "Ty" is a student at Lowell High School. C.V. stated that he heard that people bring their accounts to "Ty" and that he is the guy with "the checks."

22. A text thread located on C.V.'s phone with "Ty" at 351-322-4889 showed that C.V. and "Ty" had been in contact since September of 2023, and that contact continued through 8:21 PM on the day of the robbery. The texts appeared to show that C.V. and "Ty" had been committing a variety of financial crimes together. One of the photos in the text thread appeared to show a "washed" check. Check washing is the process of altering a stolen check so that funds may be deposited into a different account, sometimes for a greater dollar amount.

23. On Thursday, April 17, 2004, the day following the robbery, a USPS Letter Carrier notified the Nashua, NH Postmaster that the white postal tub, which is normally placed in the bottom of a blue collection box to catch mail, was missing from the blue collection

box located at the Bright Spot convenience store, 43 Dunstable Rd. Nashua, NH 0306. This collection box is located approximately 1.2 miles from Blacksmith Way, Nashua, NH, where the robbery occurred the day prior. From previous investigations, Inspectors know it is common for suspects who have obtained USPS Arrow keys to attempt to use them in the proximity of where they are taken. Additionally, Inspectors know that the missing tub is often connected to the use of an arrow key. With the rear of the collection box open, to be expeditious and avoid being interdicted by law enforcement, targets often take the whole tub and all the mail it contains.

24. Records obtained from Cellco Partnership dba Verizon Wireless, for phone number 351-322-4889, the number which C.V. had identified as connected to "Ty," showed that the number was associated with a Verizon reseller. Resellers are businesses that utilize the Verizon network to provide service for their customers. As such, Verizon does hold some of the records requested but the subscriber information is held by the reseller. For this phone number, Cellco Partnership dba Verizon Wireless identified the reseller as Comcast/Xfinity Mobile.

25. Records obtained from Comcast identified the subscriber of the account for phone number 351-322-4889 as Julio Angel Savinon ("JULIO"), 14 Watson St. Apt. 3 Lowell, MA. Comcast specifically identified the device associated with phone number 351-322-4889 as an Apple iPhone 14, bearing an IMEI of 350928999042110. In addition to phone number 351-322-4889, Comcast identified nine other phone numbers associated with that account.

26. After identifying the Comcast account subscriber as JULIO, Inspectors contacted Lowell, MA Police to see if they had any contacts with JULIO. Lowell Police records listed JULIO as residing at 14 Watson St. Unit 3 Lowell, MA 01851. Lowell Police records

showed JULIO with a date of birth of December 10, 1982, and a phone number of 978-885-8706. The number Lowell Police had listed for JULIO was one of the nine associated numbers identified by Comcast.

27. Based on JULIO's age and likely use of a different phone number, investigators conducted research to attempt to identify additional family members of JULIO, specifically looking to identify if he had any children who could fit C.V. and JANVIER's description of "Ty." Utilizing a paid database, which searches and analyzes publicly available internet data and social media, investigators located information that JULIO was associated to a Tyler SAVINON ("SAVINON") with a listed age of 18. A search of SAVINON in the same database identified a connection to phone number 351-322-4889 and a possible date of birth of April 6, 2006.

28. Utilizing the name Tyler SAVINON and the possible date of birth of April 6, 2006, investigators conducted a query of the Massachusetts Registry of Motor Vehicle records. Those records identified an active Massachusetts's driver's license belonging to Tyler Angel SAVINON, date of birth of April 6, 2006, of 14 Watson St. Apt. 3 Lowell, MA. The license was issued on April 8, 2024, and expires April 6, 2029. SAVINON is listed as 5'7" on his license.

29. SAVINON's license photograph is consistent with C.V.'s description of "TY" being a Hispanic male, with curly hair, skinny, and 5'7". Additionally, SAVINON is consistent with JANVIER's description of the "unknown male" as light skinned, possibly Puerto-Rican, approximately 17 to 18 years old, 5'7", skinny, and with a small mustache. Additionally, both C.V. and JANVIER stated that "Ty"/ "the unknown male" lived in Lowell, MA. SAVINON lives in Lowell, MA and his residence is approximately .2 miles

from Olivera Park, on Newhall St. in Lowell, where both C.V. and JANVIER stated they met with him to exchange the stolen Arrow key.

30. Investigators also reviewed records obtained from Snapchat, dba Snap Inc., for username t5Xyy. C.V. had identified this username as being associated with "Ty." That information showed that on April 19, 2024, three days after the robbery, "Ty" changed his username from t5xyy to johndoe87911. A previous username of tylers178 was also identified. Snap Inc. listed the phone number connected to the Snapchat account as 351-224-4889, the number identified by C.V. and connected to SAVINON.

31. On May 27, 2024, USPIS learned from the Nashua, NH Post Office that a customer reported a check being stolen. The customer advised the suspect altered the payee's name, amount, and attempted to deposit the check via mobile deposit. The customer advised USPS that the check, written on a St. Mary's Bank account and dated April 16, 2024, was deposited in the blue collection box outside the Bright Spot.

32. St. Mary's Bank provided a copy of the mobile deposited check which listed the payee as Miranda Grace Remo Bada, with a bank of first deposit of Bank of America ("BOA"). According to BOA records, on or about April 24, 2024, check number 1159, dated April 16, 2024, in the amount of $3,190 was remote deposited into BOA account ending in 3202. The check was written off a St. Mary's Bank account belonging to J.B., the same name as the victim who first reported the theft of his check to the Nashua Postmaster.

33. BOA collects geolocation information during the course of online banking activity. BOA also captures Internet Protocol addresses ("IP" addresses) and assigns a mobile device identifier once a mobile device successfully logs into a BOA account. Because every device that connects to the internet must use an IP address, IP address information can help to identify which computers or other devices were used to access an account.

34. According to BOA's online activity records for account ending in 3202, on April 23, 2024, a successful login was made into this account from IP 73.149.28.201, at 11:00PM, with a device ID of 1002522635. BOA's geolocation systems identified this IP as being located in the Lowell, MA area and with Comcast as the provider.

35. Additionally, that same IP, 73.149.28.201, successfully logged into the account ending in 3202, at 11:44PM on April 23, 2024, and at 12:04AM, on April 24, 2024. The device ID for both logins was 1002522635.

36. According to BOA's online activity records for account ending in 3202, on April 24, 2024, a successful login was made into this account from IP 174.242.135.83 at 12:18AM, device ID of 1002522635, the same device ID which was connected to the previous logins via Comcast IP 73.149.28.201. BOA's systems identified this IP as belonging to Verizon Wireless. This is the login for the mobile deposit of check number 1159.

37. BOA queried its records for Comcast IP 73.149.28.201 and found since January of 2024 that IP had been utilized 54 times to log in with five additional device IDs. Those device IDs were:

partyid	onlineid	deviceid
15041402111	**mirbada18**	**1002522635**
20077024409	supersavi10	571625467
20074655553	agil4039	845919276
10090512167	bebo06	1010661115
10090512167	bebo06	1010658097
20074655553	agil4039	945762807

Two of the online IDs, agil4039 and bebo06, connected multiple devices, resulting in them having two Device IDs being assigned to each Online ID, or customer ID. BOA systems geolocated all 54 of those logins to the Lowell, MA area.

38. On July 20, 2024, USPIS was notified of an alarm activation on one of the collection boxes outside the Nashua, NH Post Office, located at 38 Spring St., Nashua, NH. The alarm system notifies USPIS when collection boxes are accessed outside of normal business hours. The Arrow key stolen during the April 16, 2024, robbery on Blacksmith Way, which was still missing, was the same series utilized to access the collection boxes outside the Nashua, NH Post Office.

39. USPIS investigators reviewed surveillance video from the Nashua, NH Post Office. The surveillance video shows two subjects, one of which is carrying a backpack, approach the collection boxes from the north, walking south. The subject with the backpack appears to access the rear of the collection box while the other subject acts as a lookout.

40. On July 26, 2024, Inspectors canvassing the area of Main St., Nashua, NH, followed up with Bank of New England, located 295 Main St. While speaking with employees at Bank of New England regarding surveillance video, Inspector Doyle was advised that Bank of New England had a customer who was a recent victim of a check fraud. The customer advised Bank of New England a check he deposited in the blue collection box outside the Nashua, NH Post Office, 38 Spring St. Nashua, on July 20, 2024, had been stolen, altered and attempted to be cashed.

DATA MAINTAINED BY THE PROVIDER

41. In my training and experience, I have learned that the PROVIDER is a company that provides cellular telephone access to the general public. I also know that providers of cellular telephone service have technical capabilities that allow them to collect and generate information about the locations of the cellular telephones to which they provide service, including E-911 Phase II data, also known as GPS data or latitude-longitude data and cell-site data, also known as "tower/face information" or cell tower/sector records.

E-911 Phase II data provides relatively precise location information about the cellular telephone itself, either via GPS tracking technology built into the phone or by triangulating on the device's signal using data from several of the provider's cell towers. Cell-site data identifies the "cell towers" (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular telephone and, in some cases, the "sector" (i.e., faces of the towers) to which the telephone connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data is typically less precise that E-911 Phase II data.

42. Based on my training and experience, I know that the PROVIDER can collect E-911 Phase II data about the location of the TARGET CELL PHONE, including by initiating a signal to determine the location of the TARGET CELL PHONE on the PROVIDER's network or with such other reference points as may be reasonably available.

43. Based on my training and experience, I know that the PROVIDER can collect cell-site data about the TARGET CELL PHONE. Based on my training and experience, I know that for each communication a cellular device makes, its wireless service provider can typically determine: (1) the date and time of the communication; (2) the telephone numbers involved, if any; (3) the cell tower to which the customer connected at the beginning of the communication; (4) the cell tower to which the customer connected at the end of the communication; and (5) the duration of the communication. I also know that wireless providers such as the PROVIDER typically collect and retain cell-site data pertaining to cellular devices to which they provide service in their normal course of business in order to use this information for various business-related purposes.

44. The requested information is likely to contain evidence of violations of Title 18 U.S.C. § 111(a)(1), Assaulting, resisting, or impeding certain officers or employees, Title 18 U.S.C. § 2114, Robbery of any person having lawful charge, control, or custody of any mail matter or of any money or other property of the United States, and 18 U.S.C. § 1704, Keys locks stolen or reproduced and other federal offenses. Information about the communications and locations of the user of the device during the relevant time periods is relevant to the crimes under investigation and to any conspiracy or solicitation to commit them.

AUTHORIZATION REQUEST

45. Based on the foregoing, I request that the Court issue the proposed search warrant, pursuant to Federal Rule of Criminal Procedure 41 and 18 U.S.C. § 2703(c).

46. I further request, pursuant to 18 U.S.C. § 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), that the Court authorize the officer executing the warrant to delay notice until 30 days after the collection authorized by the warrant has been completed. There is reasonable cause to believe that providing immediate notification of the warrant may have an adverse result, as defined in 18 U.S.C. § 2705. Providing immediate notice to the subscriber or user of the TARGET CELL PHONE would seriously jeopardize the ongoing investigation, as such a disclosure would give that person an opportunity to destroy evidence, change patterns of behavior, notify confederates, and flee from prosecution. See 18 U.S.C. § 3103a(b)(1). This investigation is expected to remain in covert status for at least 30 days following the collection of the data. As further specified in Attachment B, which is incorporated into the warrant, the proposed search warrant does not authorize the seizure of any tangible property. See 18 U.S.C. § 3103a(b)(2). Moreover, to the extent that the warrant authorizes the seizure of any wire or electronic

communication (as defined in 18 U.S.C. § 2510) or any stored wire or electronic information, there is reasonable necessity for the seizure for the reasons set forth above. See 18 U.S.C. § 3103a(b)(2).

47. I further request that the Court direct the PROVIDER to disclose to the government any information described in Attachment B that is within the possession, custody, or control of the PROVIDER. I also request that the Court direct the PROVIDER to furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the information described in Attachment B unobtrusively and with a minimum of interference with the PROVIDER's services, including by initiating a signal to determine the location of the TARGET CELL PHONE on the PROVIDER's network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The government shall reasonably compensate the PROVIDER for reasonable expenses incurred in furnishing such facilities or assistance.

48. I further request that the Court authorize execution of the warrant at any time of day or night, owing to the potential need to locate the TARGET CELL PHONE outside of daytime hours.

49. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

/s/ Sean P. Doyle
Inspector Sean P. Doyle
United States Postal Inspection Service

The affiant appeared before me by telephonic conference on this date pursuant to Fed. R. Crim. P. 4.1 and affirmed under oath the content of this affidavit and application.

Date: **Aug 21, 2024**
Time: **11:32 AM**

Talesha Saint-Marc
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

1. The cellular telephone assigned call number 351-322-4889 (the "TARGET CELL PHONE"), and the account associated therewith (the "SUBJECT ACCOUNT"). The information is in the custody or control of Verizon Wireless (the "Provider"), a wireless telephone service provider headquartered at 180 Washington Valley Road, Bedminster, NJ.

2. Records and information associated with the TARGET CELL PHONE that are within the possession, custody, or control of the Provider: including information about the location of the TARGET CELL PHONE if it is subsequently assigned a different call number.

ATTACHMENT B

Particular Things to be Seized

I. Information to be Disclosed by the Provider

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any information that has been deleted but is still available to the Provider or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose to the government the following information pertaining to the SUBJECT ACCOUNT listed in Attachment A:

a. The following historical information about the customers or subscribers associated with the SUBJECT ACCOUNT during the dates of April 15-17, 2024; April 23-25, 2024; and July 19, 2024 to August 20, 2024:

i. Names (including subscriber names, user names, and screen names);

ii. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);

iii. Local and long distance telephone connection records;

iv. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions;

v. Length of service (including start date) and types of service utilized;

vi. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"); Mobile Identification Number ("MIN"), Subscriber Identity Modules ("SIM"), Mobile

Subscriber Integrated Services Digital Network Number ("MSISDN"); International Mobile Subscriber Identity Identifiers ("IMSI"), Wi-F, or International Mobile Equipment Identities ("IMEI");

vii. Other subscriber numbers or identities (including the registration Internet Protocol ("IP") address); and

viii. Means and source of payment for such service (including any credit card or bank account number) and billing records.

ix. RTT records, PCMD records, NELOS records, TrueCall records, and all other records containing timing advance measurements and distance-to tower measurements for all technologies (CDMA, GSM, UMTS, LTE, etc.); and

x. Internet activity reports, records of Internet Protocol (IP) usage, etc.

b. All records and other information (not including the contents of communications) relating to wire and electronic communications sent or received by the SUBJECT ACCOUNT during the dates of April 15-17, 2024; April 23-25, 2024; and July 19, 2024 to August 20, 2024:

i. the date and time of the communication, the method of the communication, and the source and destination of the communication (such as the source and destination telephone numbers (call detail records), email addresses, and IP addresses); and

ii. information regarding the cell tower and antenna face (also known as "sectors") through which the communications were sent and received.

iii. E-911 Phase II data;

iv. GPS data;

v. Latitude-longitude data; and

vi. Other precise location information;

c. Prospective information associated with each communication to and from the SUBJECT ACCOUNT for a period of 45 days forward from the date of service of this warrant, during all times of day and night, including:

i. Any unique identifiers associated with the cellular device, including ESN, MEIN, MSISDN, IMSI, SIM, or MIN;

ii. Source and destination telephone numbers;

iii. Date, time, and duration of communication; and

iv. All data about the cell towers (i.e. antenna towers covering specific geographic areas) and sectors (i.e. faces of the towers) to which the TT will connect at the beginning and end of each communication.

v. E-911 Phase II data;

vi. GPS data;

vii. Latitude-longitude data; and

viii. Other precise location information.

To the extent that the information described above in Attachment A is within the possession, custody, or control of the Provider, including any information that has been deleted but is still available to the Provider or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the information to the government. In addition, the Provider must furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the Location Information unobtrusively and with a minimum of interference with the Provider's services, including by initiating a signal to determine the location of the

TARGET CELL PHONE on the Provider's network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The government shall compensate the Provider for reasonable expenses incurred in furnishing such facilities or assistance.

This warrant does not authorize the seizure of any tangible property. In approving this warrant, the Court finds reasonable necessity for the seizure of the Location Information. See 18 U.S.C. § 3103a(b)(2).